AF/2700

PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/302,608
Filing Date	4/30/1999
First Named Inventor	Gu
Art Unit	2132
Examiner Name	Lanier, Benjamin E.
Attorney Docket Number	TI-28444

Total Number of Pages in This Submission

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Alan Lintel
Signature	
Date	9/19/03

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Alan Lintel		
Signature		Date	9/18/03

PTO/SB/17 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 320

Complete if Known	
Application Number	09/302,608
Filing Date	4/30/1999
First Named Inventor	Gu
Examiner Name	Lanier, Benjamin E.
Art Unit	2132
Attorney Docket No.	TI-28444

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 20-0668

Deposit Account Name: Texas Instruments Incorp

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below	Fee Paid
Total Claims	-20** =		X		=
Independent Claims	- 3** =		X		=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	320
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,300	2453	650	Petition to revive - unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 320

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Alan Lintel	*Registration No. (Attorney/Agent)*	32,478	*Telephone*	972-664-9595
Signature				*Date*	9/18/03

WARNING: Information this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

#14
1 of 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Gu	Group Art Unit: 2132
Application No.: 09/302,608	Examiner: Lanier, Benjamin E.
Filed: April 30, 1999	I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231 on 9/18/03.
Title: Pseudo-Noise Sequence Having Insertion of Variant Length and Position	Name 9/18/03 Date
Attorney Docket No.: TI-28444	

Mail Stop Appeal Briefs - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF

Dear Sir:

Appellant respectfully presents his brief in support of his appeal of the final rejection of claims in this case. The Notice of Appeal was filed on July 18, 2003.

I. Real Party in Interest

The real party in interest in this application is Texas Instruments Incorporated.

II. Related Appeals and Interferences

The undersigned is not aware of any appeals or interferences that will directly affect or have a bearing on, or be directly affected by, the Board's decision in this appeal.

III. Status of the claims

Claims 1-19 were finally rejected in the Office Action of March 18, 2003 under U.S.C. § 103(a), and are the subject of the present appeal.

IV. Status of Amendments

No amendments are pending. The claims on appeal are presented in the Appendix to Appellant's Brief.

V. Summary of the Invention

The present invention is directed towards a method of and apparatus for encrypting a digital signal. Pseudo-noise sequences, or portions thereof, are concatenated to generate an augmented pseudo-noise sequence. A data stream is encrypted using the augmented pseudo-noise sequence.

The present invention addresses a significant problem in the field of communication, in particular, in the field of wireless communications, where the security of data and voice transmissions is very important. If the polynomial used to generate a pseudo-noise sequence can be derived, the security of a transmission will be compromised.

The present invention provides encryption of data which would be extremely difficult to decrypt without knowledge both the polynomial for generating the pseudo-noise (PN) sequences and the how the multiple pseudo-noise sequences are concatenated together. The generation of the concatenated pseudo-noise sequences and the decryption of the encrypted data stream responsive to the concatenated pseudo-noise sequences can be performed without additional complex circuitry.

VI. Issues

Are claims 1 – 19 novel and unobvious over U.S. Pat. No. 4,776,012 to Zscheile, Jr. (hereinafter "Zscheile") in view of "Applied Cryptography, Second Edition", to Schneier (hereinafter "Schneier")?

VII. Grouping of the Claims

Claims 1-3, 7-8, 10-12, and 16-18 stand or fall together. Claims 4-6 and 13-15 stand or fall together. Claims 9 and 19 stand or fall together.

VIII. Argument

A. The rejection

The Examiner has finally rejected claims 1-19 under 35 U.S.C. §103 as being unpatentable over U.S. Pat. No. 4,776,012 to Zscheile, Jr. in view of "Applied Cryptography, Second Edition", to Schneier (hereinafter "Schneier").[1] With respect to claims 1 and 10, the Examiner argues:

> Zscheile, Jr. discloses an apparatus and a method for generating a plurality of PN codes and combining those PN code to produce a composite PN code (Abstract). Zscheile does not disclose that a random sequence generator would be useful in cryptography. Schneier teaches that random sequence generators are used widely in cryptography to encrypt a data stream (Page 421-422). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a random sequence generator for cryptographic purposes as taught in Schneier in order to generate a random encryption key that cannot be reproduced.[2]

With regard to claims 2, 3 and 11, the Examiner notes that Zscheile, Jr. discloses an apparatus that is capable of generating three PN codes, citing column 2, lines 24-34.[3] With regard to claims 4-6 and 13-15, the Examiner states that Zscheile, Jr. discloses a code combiner to produce a composite PN code (Abstract) where a method of inhibiting the clock which drives the composite PN generator to advance or retard the composite

---

[1] Office Action of 3/18/03.

[2] Office Action of 3/18/03, page 3.

[3] Office Action of 3/18/03, page 3.

code any desired number of phase positions (Col. 1, lines 46-52). Each individual PN generator also has its own timing gates which can be inhibited in order to jump the PN code a desired number of phase positions (Abstract).[4]

With regard to claims 7 and 17, the Examiner states that Zscheile, Jr. discloses a composite code generator apparatus for inhibiting the number of clock system pulses being employed to drive the component code generators by a number of pulses so to control the phase position of the composite code (Col. 1, lines 57-64).[5] With regard to Claim 16, the Examiner states that Zscheile Jr. discloses an exclusive OR gate to combine component PN codes (Col. 2, line 21).[6] With regard to claims 8, 9, 18 and 19, The Examiner contends that Zscheile, Jr. discloses synchronized clock pulses to the composite PN code generator that may inhibit the PN code a certain number of pulses (Abstract).[7]

B. Appellant's Argument

Claims 1-3, 7-8, 10-12, and 16-18

Applicant respectfully submits that claims 1-3, 7-8, 10-12, and 16-18 are novel and unobvious over the combination of Zscheile, Jr. in view of Schneier. Specifically, Applicant contends that neither the Zscheile, Jr. nor Schneier references disclose or make obvious the creation of an augmented pseudo-noise sequence formed as the concatenation of two or more separate pseudo-noise sequences.

Schneier merely discloses that a pseudo-noise sequence can be used to encrypt a data stream. The focus of the present application is to generate a pseudo-noise sequence which cannot be easily determined by unauthorized persons, without adding significant complex circuitry to the encrypting or decrypting devices.

Zscheile, Jr. is provided by the Examiner to show "generating a plurality of PN codes and *combining* those PN codes to produce a composite PN code." [emphasis added]. However, independent claims 1 and 10 specifically state that pseudo-noise

---

[4] Office Action of 3/18/03, page 3.

[5] Office Action of 3/18/03, page 3.

[6] Office Action of 3/18/03, page 4.

[7] Office Action of 3/18/03, page 4.

sequences, or portions thereof, are *concatenated* to generate an augmented pseudo-noise sequence.

In Zscheile, Jr., an inverting modulo two adder 10 is used to combine component PN codes from PN generators 12, 14 and 16 to produce a composite PN code on the output line 11. If the lengths of the individual codes from the PN generators 12, 14, and 16 are X, Y and Z, the composite code will have a length of X*Y*Z.[8] Figures 2A through 2D of Zscheile, Jr., show the logical combination of three PN sequence streams. In Figures 2A through 2C, the outputs of three PN sequence generators are shown. Figure 2D shows the inverted modulo-two additions of the outputs of the three PN sequence generators (i.e., if there are an odd number of "1"s generated by the PN sequence generators, output line 11 is set to "0"; else, output line 11 is set to "1"). It should be noted that once the PN sequences from the generators 12, 14 and 16 are set, the composite PN sequence is deterministic.

Zscheile, Jr. is directed towards jumping within the composite code quickly to synchronize the composite code on output line 11 with a code being received. This is accomplished by setting the numbers in the preset counters 24, 25 and 26 to vary the sequence position in the PN generators 12, 14 and 16, respectively.[9]

Concatenating two or more PN sequences, or portions thereof, as claimed in independent claims 1 and 10 is shown in Figure 1 of the present application. An augmented PN sequence 10 is generated by concatenating (1) a first portion of a first PN sequence (PN0 12), (2) a segment 16 of a second PN sequence (PN1 14), and (3) the remaining portion of the first PN sequence.

The Examiner merely argues that Zscheile, Jr. discloses generating a PN sequence by *combining* multiple PN sequences. The Examiner argues that "the applicant's argument that the cited references do not disclose concatenating a plurality of component PN sequences is not persuasive because the Zscheile, Jr. reference meets the definition of 'concatenation' since it discloses two or more sequences being combined (Abstract)."[10]

---

[8] Figure 1, Zscheile, Jr., column 2, lines 20-34.

[9] Zscheile, Jr., column 2, lines 50-56.

[10] Office Action of 3/18/03, page 2.

Applicant strongly disagrees that Zscheile, Jr. shows concatenation merely by stating that two or more PN sequences may be "combined". The Encarta World English Dictionary defines "concatenate" (with regard to computing) as:

> link units together: to link two or more information units, such as character strings or files, so that they form a single unit.[11]

Zscheile, Jr. simply does not show any combination of PN sequences that could be classified as concatenation. Performing a modulo two addition, or other logical operation, using multiple data streams as an input source, is a *transformation*, not a *concatenation*. The composite PN sequence of Zscheile would bear no resemblance to any of the individual PN sequences generated by the component PN sequence generators 12, 14 and 16, as is clear from Figures 2A through 2D of Zscheile, Jr.

Accordingly, Applicant contends that the Examiner is providing a meaning to "concatenate" which is broader that the normal meaning of the word as known by those skilled in the art. If "concatenate" is defined in accordance with its normal usage in the art of computing, the Zscheile, Jr. reference neither discloses the concatenation of multiple PN sequences to form an augmented PN sequence, nor discloses subject matter that would make obvious the concatenation of multiple PN sequences to form an augmented PN sequence.

Claims 4-6 and 13-15

Claims 4-6 and 13-15 provide more specific implementations of concatenating multiple PN sequences to generate an augmented PN sequence. In claims 4 and 13, a segment of a first PN sequence is inserted into a second PN sequence at an arbitrary position in the second PN sequence. In claims 5 and 14, the segment has an arbitrary length. In claims 6 and 15, the segment has arbitrary starting and ending positions within the first PN sequence.

With regard to these claims, the Examiner contends that Zscheile, Jr. discloses a code combiner to produce a composite PN code (Abstract) where a method of inhibiting the clock which drives the composite PN generator to advance or retard the composite code any desired number of phase positions (Col. 1, lines 46-52). Each individual PN

---

[11] Amendment After Final, filed 6/23/03.

generator also has its own timing gates which can be inhibited in order to jump the PN code a desired number of phase positions (Abstract).[12]

It is important to note that the features of Zscheile, Jr. cited by the Examiner in connection with claims 4-7 and 13-15, are not features which affect the composite PN sequence on output 11. As noted above, the composite PN sequence of Zscheile, Jr. is fixed by the outputs of the PN sequence generators 12, 14, and 16. Inhibiting the clock 18 to the counters 24, 38 and 39 jumps the output 11 to a different position in the composite PN sequence. In fact, this is the entire purpose of the Zscheile, Jr. device – to quickly jump to new position of the composite PN sequence for purposes of synchronizing the internally generated composite PN sequence to the data being received. The composite PN sequence, however, is not changed.

By contrast, the subject matter of claims 4-6 and 13-15 provides the ability to change the augmented PN sequence without changing the PN sequences that are used to generate the augmented PN sequence. The claims provide factors that make determination of the augmented PN sequence nearly impossible because of the many variations that could be used to form augmented PN sequence. To determine the augmented PN sequence, an unauthorized recipient would need to determine the polynomial used for the first PN and second PN sequences, determine the point of insertion into the second PN sequences (claims 4 and 13), determine the length of the segment to be taken from the first PN (claims 5 and 14), and determine the starting and stopping positions of the segment within the first PN sequence (claims 6 and 15).

Since Zscheile, Jr. does not show any means for changing the composite PN sequence, it cannot show the subject matter of claims 4-6 and 13-15.

Claims 9 and 19

Claims 9 and 19 provide for synchronizing the augmented PN sequence to a reference clock relative to an arbitrary offset. For example, in Figure 2 of the present application, a reference clock REF_CT provides a count for each word of a sequence. The first word of the augmented PN sequence does not necessarily start at count "0"; this first word may be generated at a count equal to "OFFSET".

---

[12] Office Action of 3/18/03, page 3.

While Zscheile, Jr. shows the ability to jump between positions, there is no counterpart to the reference clock of claim 9 and 19 where the PN sequence is synchronized to the clock.

Conclusion

For the foregoing reasons, Appellant submits that all of the claims on appeal in this case are novel and non-obvious over the prior art of record in this case. Appellant therefore respectfully submits that the final rejection of claims 1 through 19 is in error. Reversal of the final rejection of the claims in this case is therefore respectfully requested.

Respectfully Submitted,

Alan W. Lintel
Attorney/Agent for Applicant(s)
Reg. No. 32478

September 18, 2003
Anderson, Levine & Lintel
14785 Preston Road
Suite 650
Dallas, Texas 75254
Tel. (972) 664-9595

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Gu Application No.: 09/302,608 Filed: April 30, 1999 Title: Pseudo-Noise Sequence Having Insertion of Variant Length and Position Attorney Docket No.: TI-28444	Group Art Unit: 2132 Examiner: Lanier, Benjamin E. I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231 on 9/18/03. Name 9/18/03 Date

Mail Stop Appeal Briefs - Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX TO APPELLANT'S BRIEF

Dear Sir:

Appellant respectfully presents the claims on appeal in this case:

1. A method of encrypting a digital signal comprising:

generating a plurality of pseudo-noise sequences;

concatenating said pseudo-noise sequences, or portions thereof, to generate an augmented pseudo-noise sequence; and

encrypting a data stream using the augmented pseudo-noise sequence.

2. The method of claim 1 wherein said generating step comprises the step of generating first and second pseudo-noise sequences.

3. The method of claim 1 wherein said generating step comprises the step of generating three or more pseudo-noise sequences.

4. The method of claim 1 wherein said concatenating step comprises the step of inserting a segment of a first pseudo-noise sequence into a second pseudo-noise sequence at an arbitrary position in said second pseudo-noise sequence.

5. The method of claim 4 wherein said segment has an arbitrary length.

6. The method of claim 4 wherein said segment has arbitrary starting and ending positions within said first pseudo-noise sequence.

7. The method of claim 1 and further comprising the step of starting the output of the augmented pseudo-noise sequence at an arbitrary position in the sequence.

8. The method of claim 1 and further comprising the step of synchronizing the augmented pseudo-noise sequence to a reference clock.

9. The method of claim 8 wherein said synchronizing step comprises the step of synchronizing the augmented pseudo-noise sequence to a reference clock relative to an arbitrary offset.

10. Apparatus for encrypting a digital signal comprising:

two or more pseudo-noise sequence generators

circuitry for concatenating said pseudo-noise sequences, or portions thereof, to generate an augmented pseudo-noise sequence; and

an encrypting circuit for correlating the augmented pseudo-noise sequence with a data stream.

11. The apparatus of claim 10 wherein said generating step comprises the step of generating first and second pseudo-noise sequences.

12. The apparatus of claim 10 wherein said two or more pseudo-noise sequence generators comprises three or more pseudo-noise sequence generators.

13. The apparatus of claim 10 wherein said concatenating circuitry comprises circuitry for inserting a segment of a first pseudo-noise sequence into a second pseudo-noise sequence at an arbitrary position in said second pseudo-noise sequence.

14. The apparatus of claim 13 wherein said segment has an arbitrary length.

15. The apparatus of claim 13 wherein said segment has arbitrary starting and ending positions within said first pseudo-noise sequence.

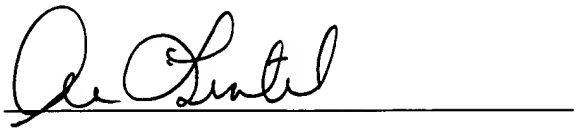
16. The apparatus of claim 13 wherein said encrypting circuit performs an exclusive-or operation.

17. The apparatus of claim 10 and further comprising circuitry for starting the output of the augmented pseudo-noise sequence at an arbitrary position in the sequence.

18. The apparatus of claim 10 and further comprising circuitry for synchronizing the augmented pseudo-noise sequence to a reference clock.

19. The apparatus of claim 18 wherein said synchronizing circuitry comprises circuitry for synchronizing the augmented pseudo-noise sequence to a reference clock relative to an arbitrary offset.

Respectfully Submitted,



Alan Lintel
Attorney/Agent for Applicant(s)
Reg. No. 32478

September 18, 2003
Anderson, Levine & Lintel
14785 Preston Road
Suite 650
Dallas, Texas 75254
Tel. (972) 664-9595